**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Ninotshka Green-Spand, Special Agent with U.S. Postal Inspection Service being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for 3646 Academy Road, Philadelphia, PA 19154 ("SUBJECT PREMISES") and a 2021 green Audi SQ5, assigned VIN #WA134BFY1M2068256, bearing Pennsylvania license plate number MRH 7929 ("SUBJECT VEHICLE").

2. I have been employed as a Postal Inspector since June 2017. I am also a Task Force Officer with the Department of Homeland Security, Cybercrimes Investigations Task Force, and have been since February 2021. Prior to becoming a Postal Inspector, I was employed as a Confidential Investigator with the Philadelphia Housing Authority for four-and-a-half years. I have a Master of Science in Criminal Justice from Saint Joseph's University in Philadelphia, PA. As part of my duties as a United States Postal Inspector, I investigate the use of the U.S. Mail to illegally transport controlled substances and drug trafficking, in violation of Title 21, United States Code, Sections 841(a)(1), 843(b), and 846. I have been trained in various aspects of law enforcement, including the investigation of narcotics offenses. Through my education and experience and that of other agents assisting in this investigation, I have become familiar with the methods that individuals use to traffic narcotics through the U.S. Mail.

3. Based on my training and experience with the USPIS, along with discussions with other agents about their experience, I have become familiar with the mechanics of the parcel delivery services and have developed a good understanding of the appeal these services have for

those who choose them for the illegal transportation of controlled substances. Parcel delivery services offer rapid and dependable service for most metropolitan areas. Parcels are guaranteed for delivery in the number of specified days, with a refund if the parcel does not meet the service standards. To the smuggler, the refund is a minor consideration, but parcels delayed beyond the normal delivery time serve to alert the recipient that the authorities may have discovered the controlled substances. Additionally, parcel delivery services use assigned label numbers, which make it easy for the parcels to be tracked. The sender is given a time of shipment, plus the weight of the parcel. Based on my training and experience, traffickers in illegal controlled substances and the proceeds of illegal controlled substances are known to use parcel services to transport their product and/or proceeds because it is relatively anonymous, secure, and fast. I also know based on my training and experience that drug traffickers will often use the United States Postal Service ("USPS"), which provides shipping services using the U.S. Mail, to transport narcotics or the proceeds from the sale of narcotics because of the anonymity it provides the sender and recipient as well as the need for law enforcement to utilize a warrant to examine domestic mail shipments.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. Based on my training and experience, your affiant also has knowledge of the following common practices utilized by drug traffickers:

a. Narcotics traffickers often conceal evidence of their drug dealing and efforts to hide and/or launder the proceeds from their drug dealing in their residences, vehicles, and stash houses. This evidence also may be found in other areas where

a drug dealer has ready access, such as rented storage areas and safety deposit boxes. This evidence includes drugs, paraphernalia for weighing, packaging, and distributing drugs, other contraband, records and evidence of drug transactions, proceeds from sales of drugs, and valuables obtained from proceeds;

b. It is common for drug traffickers to secrete narcotics, firearms, ammunition, proceeds of drug sales, records of drug transactions, and drug paraphernalia (including grinders, scales, ink pads, stamps, razor blades, mirrors, vials, kilo presses, vacuum sealers, plastic wrap for a vacuum sealer, freezer bags, plastic baggies, paper bindles, balloons, wrapping paper, cellophane, and film canisters, and cutting agents and diluents) in secure locations within their vehicles, residences, or stash locations for ready access and to conceal them from law enforcement authorities;

c. Narcotics traffickers often maintain records of their transactions in their residences, vehicles, stash houses and other locations used to facilitate drug trafficking. These records can memorialize past transactions, the status of accounts receivable and accounts payable, and the names and contact information of suppliers, customers, and co-conspirators. Records frequently include the identification of properties such as real property or vehicles owned, rented, leased, controlled, or otherwise utilized by the trafficker and his co-conspirators in the distribution of controlled substances. These records include property rental and ownership records such as deeds of trusts and lease and purchase agreements, and vehicle registration, rental, and ownership information;

d. Narcotic traffickers may use the internet through their personal computers or hand-held wireless devices to communicate with other traffickers, suppliers, customers, and to order packaging materials and paraphernalia; drug traffickers may use facsimile machines to place or receive orders from customers and suppliers and to order packaging materials and paraphernalia for their drug activities; and narcotics traffickers may also maintain records of their drug trafficking transactions and activities in electronic files stored within their personal computers or hand-held wireless devices. Traffickers also use the dark web to sell and negotiate the sale of narcotics. They use storage devices, laptops, and portable drives to conceal their online presence and facilitate the sale of narcotics.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Section 846 (conspiracy to distribute a controlled substance); and Title 21, United States Code, Section 841(a)(1) (distribution and possession with intent to distribute a controlled substance); have been committed, are being committed, and will be committed by Steven Simpson who resides at 3646 Academy Rd, Philadelphia, PA 19154 ("SUBJECT PREMISES") and that Simpson uses the SUBJECT VEHICLE to commit the above listed offenses.

## PROBABLE CAUSE

5. On March 14, 2025, USPIS, Pittsburgh Division, Cleveland Domicile ("hereinafter USPIS Cleveland"), contacted USPIS in Philadelphia regarding a fatal overdose that occurred on March 4, 2025, in Canton, Ohio. It appeared the fatal overdose was likely caused by drugs originally contained inside a USPS parcel, further described as USPS Priority

Mail Express parcel bearing tracking no. "9470 1362 0832 6274 3977 64" addressed to "RIAN ROSS, 305 22ND ST NW, CANTON, OH 44709-3901," and bearing a return address of EBAY COLLECTION, 709 N 2ND ST STE 400, PHILADELPHIA, PA 19123-3108 (hereinafter "Canton Parcel"). The Canton Parcel was mailed from Philadelphia, Pennsylvania, on March 3, 2025, and delivered on March 4, 2025, to the victim's address in Canton.

6. USPS business records queries determined the Canton Parcel was purchased through a third-party postage provider. Based on previous narcotics seizures using similar postage, USPIS knew this third-party postage provider is commonly used by individuals who mail illicit controlled substances via the USPS. Through further USPS business records queries, USPIS Cleveland discovered a customer associated with the postage provider, Kody Kepler.

7. Through additional USPS business records queries, USPIS Cleveland learned that the name Kody Kepler was associated with at least three USPS customer accounts located in Philadelphia, PA: (1) User ID 403936568 with User Name Ckepler6284, Name Kody Kepler, Company Name KEEPS LLC, Address 737 Bainbridge St Apt 36, Philadelphia, PA 19147, Phone Number 443-681-9147, Email ckepler6284@gmail.com, (2) User ID 395594544 with User Name KEEPS_LLC, Name Kody Kepler, Company Name TABLESCAPE, Address 737 Bainbridge St, Philadelphia, PA 19147, Phone Number 215-327-0914, Email kodykepler@outlook.com, and (3) User ID 398098308 with User Name TABLESCAPELLC, Name Kody Kepler, Company Name TABLESCAPE LLC, Address 737 Bainbridge St, Philadelphia, PA 19147, Phone Number 215-327-0914, Email silviaskyy@keemail.me.

8. Through additional USPS business records queries, USPIS Cleveland learned that email silviaskyy@keemail.me is also associated with the USPS customer account with User ID 426423935 and User Name academyrd, Name: Steven Simpson, Company Name SBS LLC,

Address 3646 Academy Rd, Philadelphia, PA 19154, Phone Number 202-394-2027, most recent login February 25, 2025, at 10:16 a.m. EST. Through queries in CLEAR, USPIS Cleveland was able to associate an individual named Steven Simpson with date of birth, credit, and banking records at the address 737 Bainbridge Street, Philadelphia, PA 19147. Since March 2023, USPS business records showed more than 40 parcels delivered to 3646 Academy Road, Philadelphia, PA 19154 that were addressed to Steven Simpson.

**Seized Parcel**

9. A USPIS business records search revealed a USPS Priority Mail seizure that occurred within USPIS Boston Division. The seizure revealed a USPS Priority Mail Parcel with tracking number 9405 5362 0832 6279 0575 51. The parcel was mailed from Philadelphia, PA and had the following characteristics:

| | |
|---|---|
| Priority Mail No.: | 9405 5362 0832 6279 0575 51 |
| Measuring approx.: | 12.5" x 9.5" |
| Weight approx.: | 3lbs[1] |
| Return Address: | Ebay Collection<br>709 N 2nd Street Ste 400<br>Philadelphia, PA 19123 |
| Delivery Address: | Colin Marcom<br>44 4th St Apt.2<br>Troy, NY 12180 |

10. The parcel was opened and found to contain 15.5 grams of white powder which tested positive for the presence of fentanyl. This is the same return address as the parcel involved in the overdose death in Ohio.

[1] This may not reflect the actual weight of the parcel. This weight amount is obtained from USPS Business records based on the information provided by the USPS postage account holder and/or mailer.

**Surveillance**

11. On March 18th, 2025, members of the HSI Cyber Task Force conducted surveillance on the SUBJECT PREMISES. At approximately 1:44 pm, a Caucasian male with a long beard exited the front door of the target residence wearing a blue and white backpack. Law enforcement identified the male as Steven Simpson. Simpson entered the SUBJECT VEHICLE and drove away from the residence. Law enforcement followed the SUBJECT VEHICLE which parked near a USPS Post Office located at 3000 Chestnut Street, Philadelphia, PA 19104. Law enforcement observed Simpson exit the SUJECT VEHICLE and enter the Post Office. Upon arriving at a silver drop box in the Post Office, Simpson opened the backpack, took out several parcels, and dropped them in the box. Simpson then exited the Post Office, returned to the SUBJECT VEHICLE and drove away from the Post Office.

12. USPIS Philadelphia arrived at the Post Office shortly thereafter and removed approximately 28 parcels from the Post Office's internal hamper on the receiving end of the drop box. USPIS Philadelphia discovered that the 28 parcels fit the profile and characteristics of the Canton Parcel and the NY Parcel.

**Seizure of Simpson's Recent Mailings**

13. On or about March 19th, 2025, the Honorable Pamela A. Carlos authorized the search of two of the seized parcels, 25-mj-587-1, 2, Priority Express Parcel # 9470 1362 0832 6274 4565 39 ("Subject Parcel One") and USPS Priority Parcel #9405 5362 0832 6284 0859 76 ("Subject Parcel Two").

14. Postal Inspectors opened Subject Parcel One and found a small white powdery brick like substance inside a clear vacuum sealed bag. The small white powdery brick like

substance field tested positive for the presence of fentanyl, a Schedule II controlled substance, and weighed approximately 14 grams.

15. Postal Inspectors opened Subject Parcel Two and found three small white powdery brick like substances inside a clear vacuum sealed bag. Two of the small bags of white powdery brick like substances field tested positive for the presence of fentanyl a Schedule II controlled substance. The combined weight of all three bags is approximately 3 grams.

**BACKGROUND REGARDING VIRTUAL CURRENCY AND DARKNET SITES**

16. Virtual Currency: Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin (or "BTC") is currently the most well-known virtual currency in use.

17. Virtual Currency Address: Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

18. Private Key: Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

19. Virtual Currency Wallet: A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at one time.

20. Blockchain: Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour, records every virtual currency address that has ever received that virtual currency, and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

21. Virtual Currency Exchanges: Virtual currency exchanges ("VCEs") are trading and/or storage platforms for virtual currencies such as BTC. Many VCEs also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (i.e., "know your customer" or "KYC" checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States or other countries with similar requirements). A U.S.-based VCE is thus required to collect identifying information of their customers and verify their clients' identities. See 31 U.S.C. § 5311 et seq. (Bank Secrecy Act).

22. Blockchain Analysis: As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (e.g., the BTC blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. For example, when an organization creates multiple BTC addresses, it will often combine its BTC addresses into a separate, central BTC address (i.e., a "cluster"). It is possible to identify a cluster of BTC

addresses held by one organization by analyzing the BTC blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction.

23. Darknet Sites: The "darknet" is a portion of the Internet, where individuals must use an anonymizing software or application in order to access content and websites. Within the darknet, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and stolen credit card data, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web"). These online market websites use a variety of technologies and techniques, to ensure that communications and transactions are shielded from interception and monitoring. Famous darknet marketplaces, also called Hidden Services, such as Silk Road, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. Payment on criminal darknet sites, is almost exclusively conducted using virtual currency.

**SIMPSON'S DARKNET VENDOR SITE**

24. On March 14, 2025, USPIS Cleveland conducted a Knock & Talk interview at the residence of Buyer #1, a USPS Customer and PO Box holder, regarding a USPS Priority mail parcel # 9405 5362 0832 6281 0738 91 ("PO Box Parcel"), " addressed to "Robert Miller, PO Box 105, Beach City, OH 44608," and bearing a return address of CK INC, 2290 W Oregon Ave, Phila, PA 19145 (hereinafter "PO Box Parcel"). The PO Box parcel was mailed from Philadelphia, PA on March 10, 2025. The PO Box parcel profile and characteristics were consistent with the other parcels recovered in this case.

25. Buyer #1 voluntarily informed USPIS Cleveland that he purchased "maja" fentanyl on a dark net market called "Archetyp." Miller showed USPIS Cleveland how he placed

the fentanyl order through his dark net account. Additionally, Miller informed USPIS Cleveland that he has placed multiple fentanyl orders from the same "Omega1" vendor on the dark net market "Archetyp."

26. USPIS Cleveland opened the PO Box Parcel and found inside a clear vacuum sealed bag with writing ".5g maja" in red, and inside a small white chunk of a powdery substance. The white powdery chunk field tested positive for fentanyl.

27. Based on this information, your affiant believes that Simpson operates or facilitates in the operating of the Omea1 vendor page. Individuals like Simpson that use the darknet, rely on encrypted peer to peer communications and virtual currency to operate and conduct drug trafficking. Based on training and experience, I know that in order to access the darknet, use encrypted peer to peer communications or conduct the virtual currency activities detailed herein, one must have access to the internet, a computer or smartphone and the specific software or application installed.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

28. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the SUBJECT PREMISES and in the SUBJECT VEHICLE, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices such as computer hard drives or other electronic storage media. Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

29. Probable cause. Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT PREMISES or SUBJECT VEHICLE, there is probable cause to believe that evidence, fruits, and/or instrumentalities of narcotics trafficking will be stored on those digital devices or other electronic storage media. As discussed herein, I believe that Simpson has used digital devices to commit violations of Title 21 United States Code Sections 841 and 846, to sell drugs via the Darknet. There is, therefore, probable cause to believe that evidence, fruits and/or instrumentalities of narcotics offenses exists and will be found on digital device or other electronic storage media at the SUBJECT PREMISES and/or SUBJECT VEHICLE, for at least the following reasons:

a Based my knowledge, training, and experience, I know that computer files or remnants of such files may be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, this information can sometimes be recovered months or years later with forensics tools. This is because when a person "deletes" a file on a computer, the data contained in the files does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in "swap" or "recovery" files.

c Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the SUBJECT PREMISES and/or SUBJECT VEHICLE because:

a Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as

the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing a user's intent.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of

how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

32. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in

order to determine whether it is evidence described by the warrant.

34. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices, and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the

device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e As discussed in this affidavit, based on my training, and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been

entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require Simpson, to unlock the device using biometric features in the same manner as discussed above.

35. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the SUBJECT PREMISES and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

## REQUEST FOR SEALING

36. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

## CONCLUSION

37. Based on the above facts, your affiant submits that there is probable cause to believe that the SUBJECT PREMISES and SUBJECT VEHICLE may contain evidence of the drug distribution activities, in violation of Title 21 United States Code, Sections 841(a)(1) and 846, and as such, a search warrant for the SUBJECT PREMISES and SUBJECT VEHICLE should be issued.

Respectfully submitted

s/_ Ninotshka Green-Spand
Ninotshka Green-Spand
U.S. Postal Inspection Service

Subscribed and sworn to before
me by telephone
this 20th day of March, 2025

BY THE COURT:

PAMELA A. CARLOS

Digitally signed by PAMELA A. CARLOS
Date: 2025.03.20 11:30:03 -04'00'

HON. PAMELA CARLOS
UNITED STATES MAGISTRATE JUDGE

# ATTACHMENT A -1

## Property to Be Searched

1. 3646 Academy Rd, Philadelphia, PA 19154 ("SUBJECT PREMISES"). The SUBJECT PREMISES is a two-story row-home residence with a front and back yard and a single driveway. The residence has white main door and storm door.

**ATTACHMENT A -2**

A 2021 green Audi SQ5, assigned VIN # WA134BFY1M2068256, bearing Pennsylvania license plate number MRH 7929 ("SUBJECT VEHICLE").

# ATTACHMENT B

## (PROPERTY TO BE SEIZED FROM SUBJECT PREMISES)

Items to be Seized

This warrant authorizes the government to search for the following evidence, fruits, and/or instrumentalities of Distribution and/or Possession of Controlled Substances with Intent to Distribute in violation of Title 21, United States Code, Section 841(a)(1) and Conspiracy to Distribute Controlled Substances in violation of Title 21, United States Code, Section 846.

1. Controlled Substances and controlled substance analogues.

2. Drug Paraphernalia and Instruments of Drug Trafficking: Items used, or to be used, to store, process, package, use, and/or distribute controlled substances; plastic bags, cutting agents, scales, measuring equipment, tape, hockey or duffel bags, chemicals or items used to test the purity and/or quality of controlled substances.

3. Drug Transaction Records: Documents such as ledgers, receipts, and notes relating to the acquisition, transportation, and distribution of controlled substances, however stored, including in digital devices.

4. Customer and Supplier Information: Items identifying drug customers and drug suppliers, such as telephone records, personal address books, correspondence, diaries, calendars, notes with phone numbers and names, “pay/owe sheets” with drug amounts and prices, and maps or directions.

5. Cash and Financial Records: Currency and financial records, such as bank records, safe deposit box records and keys, credit card records, bills, receipts, tax returns, and vehicle documents; records that show income and expenditures, net worth, money transfers, wire transmittals, negotiable instruments, bank drafts, and cashier’s checks.

6. Photographs/Video: Photographs, video tapes, digital cameras, surveillance

cameras, and associated hardware/storage devices depicting property occupants, friends and relatives of the property occupants, or suspected buyers or sellers of controlled substances, controlled substances or other contraband, weapons, and assets derived from the distribution of controlled substances.

7. Codes: Evidence of codes used in the distribution of controlled substances, such as passwords, code books, cypher or decryption keys.

8. Property Records: Deeds, contracts, escrow documents, mortgage documents, rental documents, and other evidence relating to the purchase, ownership, rental, income, expenses, or control of the SUBJECT PREMISES, and similar records of other property owned or rented.

9. Indicia of occupancy, residency, and/or ownership of assets such as utility and telephone bills, canceled envelopes, rental records or payment receipts, leases, and mortgage statements.

10. Evidence of storage unit rental or access such as rental and payment records, keys and codes, pamphlets, contracts, contact information, directions, and passwords.

11. Evidence of Personal Property Ownership: Registration information, ownership documents, or other evidence of ownership of personal property such as vehicles and jewelry; evidence of international or domestic travel, hotel stays, and other evidence of unexplained wealth.

12. Individual and business financial books, records, receipts, notes, ledgers, diaries, journals, and all records relating to income, profit, expenditures, or losses, such as:

a. Employment records: paychecks or stubs, lists and accounts of employee payrolls, records of employment tax withholdings and contributions, dividends, stock certificates, and compensation to officers.

b. Savings accounts: statements, ledger cards, deposit tickets, register records, wire transfer records, correspondence, and withdrawal slips.

c. Checking accounts: statements, canceled checks, deposit tickets, credit/debit documents, wire transfer documents, correspondence, and register records.

d. Loan Accounts: financial statements and loan applications for all loans applied for, notes, loan repayment records, and mortgage loan records.

e. Collection account statements and other-related records.

f. Certificates of deposit: applications, purchase documents, and statements of accounts.

g. Credit card accounts: credit cards, monthly statements, and receipts of use.

h. Receipts and records related to gambling wins and losses, or any other contest winnings.

i. Insurance: policies, statements, bills, and claim-related documents.

j. Financial records: profit and loss statements, financial statements, receipts, balance sheets, accounting work papers, any receipts showing purchases made, both business and personal, receipts showing charitable contributions, and income and expense ledgers.

k. Information and records about virtual currencies, including wallets, exchange information or records relating to virtual currency transactions.

13. All Western Union and/or Money Gram documents and other financial documents evidencing domestic or international wire transfers, money orders, official checks, cashier's checks, or other negotiable interests that can be purchased with cash, including applications, payment records, money orders, and frequent customer cards.

14. Negotiable instruments, jewelry, precious metals, and financial instruments.

15. Documents reflecting the source, receipt, transfer, control, ownership, and disposition of United States and/or foreign currency.

16. Correspondence, papers, records, and any other items showing employment or lack of employment.

17. Safes and locked storage containers, and the contents thereof which are otherwise described in this document.

18. Tools that may be used to open hidden compartments in vehicles, such as paint, bonding agents, magnets, or other items that may be used to open/close said compartments.

19. Digital computing devices, e.g., desktop and laptop computers and table devices; digital storage devices, e.g., external hard drives and USB thumb drives, and; optical and magnetic storage media, e.g., Blue Ray discs, DVDs and CDs.

20. Cell Phones and other digital communication devices for evidence, fruits, and/or instrumentalities of the above-referenced crimes, for the date range of January 1, 202t through today's date specifically for:

a. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);

b. Stored list of recent received, sent, or missed calls;

c. Stored contact information;

d. Stored photographs and videos of narcotics, currency, financial records (such as deposit slips and other bank records), RVs and other vehicles, firearms or other weapons, evidence of the aforementioned crimes of investigation, and/or that may show the user of the phone and/or coconspirators, including any embedded GPS data associated with these photographs; and

e. Stored text messages that are evidence of the above-listed federal crimes or that may identify the user of the seized phones and/or coconspirators, including messages sent via messaging apps, including Wickr, Signal, WhatsApp, and Telegram, or other similar messaging services where the data is stored on the telephone.

21. During the execution of the search of the SUBJECT PREMISES and SUBJECT VEHICLE described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Simpson, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.